Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for using parental controls, the method comprising:

storing parental control information on a user device;

receiving a request from the user device to access a destination over a communications network;

using the parental control information stored on the user device to determine whether to grant the request from the user device;

allowing the user device access to the destination when the parental control information indicates that the request should be allowed;

denying the user device access to the destination when the parental control information indicates that the request should be denied;

storing on a remote device information that is related to the parental control information stored on the user device;

using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device; and

if the parental control information stored on the user device has been altered without authorization of the master account holder for the user device:

replacing the altered version of the parental control information stored on the user device with an unaltered version of the parental control information, and

sending a message to the master account holder for the user device, the message indicating that the parental controls stored on the user device have been altered without authorization of the master account holder for the user device.

2. (Previously Presented) The method as in claim 1 wherein the information stored on the remote device includes a checksum of a version of the parental control information stored on the user device and using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device includes verifying the parental control information stored on the user device using the checksum stored on the remote device.

3. (Previously Presented) The method as in claim 1 wherein the information stored on the remote device includes a copy of a version of the parental control information stored on the user device and using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device includes verifying the parental control information stored on the user device using the copy of the parental control information stored on the remote device.

4. (Previously Presented) The method as in claim 1 wherein the information stored on the remote device includes a checksum and a copy of the parental control information stored on the user device and using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device includes verifying the parental control information stored on the user device using the checksum or the copy of the parental control information stored on the remote device.

5. (Cancelled).

6. (Previously Presented) The method as in claim 1 wherein using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization comprises doing so periodically.

7. (Previously Presented) The method as in claim 1 wherein using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization comprises doing so based on an occurrence of an event.

8. (Previously Presented) The method as in claim 3 wherein:

the parental control information stored on the user device includes a checksum computed from the version of the parental control information stored on the user device for the parental controls, and

using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device includes comparing the checksum stored on the remote device with the checksum stored on the user device.

9. (Cancelled).

10. (Cancelled).

11. (Previously Presented) The method as in claim 3 wherein using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device includes comparing the copy of the parental control information stored on the remote device with the parental control information stored on the user device.

12. (Cancelled).

13. (Cancelled).

14. (Previously Presented) The method as in claim 1 wherein the parental control information includes parental control information that is based on age-appropriateness of a content.

15. (Previously Presented) The method as in claim 1 wherein the parental control information is indicative of an identity that is signed into the user device.

16. (Original) The method as in claim 1 wherein the communications network includes the Internet.

17. (Original) The method as in claim 1 wherein the destination includes a web site.

18. (Previously Presented) A system for using parental controls, comprising:
at least one processor;
a computer-readable storage medium storing a computer program comprising:
a user device storing code segment that causes the processor to store parental control information on a user device;
a receiving code segment that causes the processor to receive a request from the user device to access a destination over a communications network;
a using code segment that causes the processor to use the parental control information stored on the user device to determine whether to grant the request from the user device;

an access code segment that causes the processor to allow the user device access to the destination when the parental control information indicates that the request should be denied;

a remote device storing code segment that causes the processor to store on a remote device information that is related to the parental control information stored on the user device; and

a verifying code segment that causes the processor to use the information stored on a remote device to determined whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device;

a replacing code segment that causes the processor to replace the altered version of the parental control information on the user device with an unaltered version of the parental control information when the parental control information stored on the user device has been altered without authorization of the master account holder for the user device, and

a notification code segment that causes the processor to sent a message to the mater account holder for the user device when the parental control information stored on the user device has been altered without authorization, the message indicating that the parental controls stored on the user device shave been altered without authorization of the master account holder for the user device.

19. (Previously Presented) The system of claim 18 wherein the information stored on the remote device includes a checksum of a version of the parental control information stored on the user device and the verifying code segment causes the computer to verify the parental control information stored on the user device using the checksum on the remote device.

20. (Currently Amended) The system of claim 18 wherein the information stored on the remote device includes a copy of a version of the parental control information stored on the user device and the verifying code segment causes the computer to verify the parental control information stored on the user device using the copy of the parental control information stored on [[teh]] the remote device.

21. (Previously Presented) The system of claim 18 wherein the information stored on the remote device includes a checksum and a copy of the parental control information stored on the user device and the verifying code segment causes the computer to verify the parental control information stored on the user device using the checksum or the copy of the parental control information stored on the remote device.

22. (Cancelled).

23. (Previously Presented) The system of claim 18 wherein using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device comprises doing so periodically.

24. (Currently Amended) The system of claim 18 wherein using the information ~~stoed~~ stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device comprises doing so based on the occurrence of an event.

25. (Previously Presented) The system of claim 20 wherein:

the parental control information stored on the user device includes a checksum computed from the version of the parental control information stored on the user device for the parental controls, and

the verifying code segment causes the computer to compare the checksum stored on the remote device with the checksum stored on the user device.

26. (Cancelled).

27. (Cancelled).

28. (Previously Presented) The system of claim 20 wherein the verifying code segment causes the computer to compare the copy of the parental control information stored on the remote device with the parental control information stored on the user device.

29. (Cancelled).

30. (Cancelled).

31. (Previously Presented) The system of claim 18 wherein the parental control information includes parental control information that is based on age-appropriateness of a content.

32. (Previously Presented) The system of claim 18 wherein the parental control information is indicative of an identity that is signed into the user device.

33. (Original) The system of claim 18 wherein the communications network includes the Internet.

34. (Original) The system of claim 18 wherein the destination includes a web site.

35. (Previously Presented) A computer-readable storage medium storing a computer program, the computer program comprising:

a user device storing code segment that causes a computer to store parental control information on a user device;

a receiving code segment that causes the computer to receive a request from the user device to access a destination over a communications network;

a using code segment that causes the computer to use the parental control information stored on the user device to determine whether to grant the request from the user device;

an access code segment that causes the computer to allow the user device access to the destination when the parental control information indicates that the request should be allowed;

a denial code segment that causes the computer to deny the user device access to the destination when the parental control information indicates that the request should be denied;

a remote device storing code segment that causes the computer to store on a remote device information that is related to the parental control information stored on the user device; and

a verifying code segment that causes the computer to use the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device;

a replacing code segment that causes the computer to replace the altered version of the parental control information stored on the user device with an unaltered version of the parental control information when the parental control information stored on the user device has been altered without authorization of the master account holder for the user device, and

a notification code segment that causes the computer to send a message to the master account holder for the user device when the parental control information stored on the user device has been altered without authorization, the message indicating that the parental controls stored on the user device have been altered without authorization of the master account holder for the user device.

36. (Previously Presented) The computer-readable storage medium of claim 35 wherein the information stored on the remote device includes a checksum of a version of the parental

control information stored on the user device and the verifying code segment causes the computer to verify the parental control information stored on the user device using the checksum stored on the remote device.

37. (Previously Presented) The computer-readable storage medium of claim 35 wherein the information stored on the remote device includes a copy of a version of the parental control information stored on the user device and the verifying code segment causes the computer to verify the parental control information stored on the user device using the copy of the parental control information stored on the remote device.

38. (Previously Presented) The computer-readable storage medium of claim 35 wherein the information stored on the remote device includes a checksum and a copy of the parental control information stored on the user device and the verifying code segment causes the computer to verify the parental control information stored on the user device using the checksum or the copy of the parental control information stored on the remote device.

39. (Cancelled).

40. (Previously Presented) The computer-readable storage medium of claim 35 wherein using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device comprises doing so periodically.

41. (Previously Presented) The computer-readable storage medium of claim 35 wherein using the information stored on the remote device to determine whether the parental control information stored on the user device has been altered without authorization of a master account holder for the user device comprises doing so based on an occurrence of an event.

42. (Previously Presented) The computer-readable storage medium of claim 37 wherein:

the parental control information stored on the user device includes a checksum computed from the version of the parental control information stored on the user device for the parental controls, and

the verifying code segment causes the computer to compare the checksum stored on the remote device with the checksum stored on the user device.

43. (Cancelled).

44. (Cancelled).

45. (Previously Presented) The computer-readable storage medium of claim 37 wherein the verifying code segment causes the computer to compare the copy of the parental control information stored on the remote device with the parental control information stored on the user device.

46. (Cancelled).

47. (Cancelled).

48. (Previously Presented) The computer-readable storage medium of claim 35 wherein the parental control information includes parental control information that is based on age-appropriateness of a content.

49. (Previously Presented) The computer-readable storage medium of claim 35 wherein the parental control information is indicative of an identity that is signed into the user device.

50. (Previously Presented) The computer-readable storage medium of claim 35 wherein the communications network includes the Internet.

51. (Previously Presented) The computer-readable storage medium of claim 35 wherein the destination includes a web site.

52. (Previously Presented) A method for using parental controls, the method comprising:

storing first parental control information on a first user device;

storing second parental control information on a second user device;

storing on a remote device information that is related to the first parental control information stored on the first user device;

storing on the remote device information that is related to the second parental control information stored on the second user device;

using the information stored on the remote device to determine whether the first parental control information stored on the first user device has been altered without authorization of a first master account holder for the first user device;

if the parental control information stored on the first user device has been altered without authorization of the first master account holder for the first user device:

replacing the altered version of the first parental control information stored on the first user device with an unaltered version of the first parental control information, and

sending a first message to the first master account holder for the first user device, the first message indicating that the first parental controls stored on the first user device have been altered without authorization of the first master account holder for the first user device; using the information stored on the remote device to determine whether the second parental control information stored on the second user device has been altered without authorization of a second master account holder for the second user device; and

if the parental control information stored on the second user device has been altered without authorization of the second master account holder for the second user device:

replacing the altered version of the second parental control information stored on the second user device with an unaltered version of the second parental control information, and

sending a second message to the second master account holder for the second user device, the second message indicating that the second parental controls stored on the second user device have been altered without authorization of the second master account holder for the second user device.